UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

GOOGLE LLC, *Plaintiff*, v. DMITRY STAROVIKOV; ALEXANDER FILIPPOV; Does 1–15, *Defendants*.	Civil Action No. 1:21-cv-10260-DLC

DECLARATION OF LAURA HARRIS IN SUPPORT OF GOOGLE LLC'S MEMORANDUM OF LAW IN OPPOSITION TO DEFENDANTS DMITRY STAROVIKOV AND ALEXANDER FILIPPOV'S MOTION TO VACATE THE ENTRY OF DEFAULT AND TO DISMISS

AND

MOTION FOR DEFAULT JUDGMENT AND PERMANENT INJUNCTION

I, Laura Harris, hereby declare and state as follows:

1. I am an attorney with the law firm of King & Spalding LLP and counsel of record for Plaintiff Google LLC ("Google"). I am a member of good standing of the bar of New York. I make this declaration in support of Google's Opposition to Defendants' Motion to Vacate and to Dismiss this Action and Google's Motion for Default Judgment and a Permanent Injunction. I make this declaration of my own personal knowledge and, if called as a witness, I could and would testify competently to the truth of the matters set forth herein.

I. Google Properly Served Defendants.

2. As described more fully below, Defendants Dmitry Starovikov, Alexander Filippov, and John Doe Defendants 1–15 ("Defendants") have been properly served with the Complaint and Exhibit A thereto, ECF No. 5; the summons; the Motion for a Temporary Restraining Order ("TRO"), ECF No. 18; the Memorandum of Law in Support of the Motion for a TRO, ECF No. 19; the Proposed TRO and Order to Show Cause Regarding a Preliminary Injunction, ECF No. 20; and all supporting evidence (collectively, the "TRO Documents") pursuant to the means authorized by the Court in the Temporary Restraining Order, ECF No. 8.

3. A true and correct copy of the Complaint and Exhibit A thereto are attached hereto as **Exhibit 1**. True and correct copies of the summons are attached hereto as **Exhibit 2**. True and correct copies of the Motion for a Temporary Restraining Order, the Proposed TRO and Order to Show Cause Regarding a Preliminary Injunction, and supporting documents are attached hereto as **Exhibit 3**. A true and correct copy of the Court's Temporary Restraining Order and Order to Show Cause is attached hereto as **Exhibit 4**. A true and correct copy of the Preliminary Injunction Order is attached hereto as **Exhibit 5**. A true and correct copy of the Huntley Declaration and supporting documents is attached hereto as **Exhibit 6**. A true and correct copy of the Bisbee

Declaration is attached hereto as **Exhibit 7**. A true and correct copy of the Harris Declaration and supporting documents is attached hereto as **Exhibit 8**.

4. In light of (a) Google's efforts to serve Defendants by physical mail, email, and text message (including by WhatsApp), (b) widespread news of this case, including in Russia, that specifically names Defendants Starovikov and Filippov and details the allegations against them, and (c) Google's disruption of the botnet's activity and Defendants' actions in response thereto, Defendants have been on notice of this action since at least December 10, 2021. Nonetheless, Defendants failed to respond or otherwise appear in this case for several months. *See* ECF Nos. 39, 40. Defendants' Motion to Vacate the Entry of Default and to Dismiss The Action followed. *See* ECF No. 41.

5. The Defendants against whom entry of default is sought are not infants or incompetent persons, and I have seen no indication that Defendants are absent or have failed to file responsive pleadings due to present military service.

II. Procedural History

6. On December 2, 2021, Google filed the Complaint in this matter and the Court entered a TRO enjoining Defendants' botnet-related activities, under seal. *See* ECF No. 8. The matter was ordered unsealed on December 6, 2021, and the Complaint and TRO were publicly filed on the docket on December 7, 2021.

7. On December 16, 2021, the Court entered a Preliminary Injunction Order. *See* Ex. 5, ECF No. 17.

8. On January 31, 2022, the Court entered a Scheduling Order requiring that Google file: a request for entry of default by February 7, 2022, and a motion for default judgment within

21 days. *See* ECF No. 33. A true and correct copy of the Scheduling Order is attached hereto as **Exhibit 9**.

9. On February 7, 2022, Google filed a request for Entry of Default, *see* ECF No. 37, and the Clerk of the Court entered a Certificate of Default on February 8, 2022, *see* ECF No. 38. A true and correct copy of Google's request for Entry of Default is attached hereto as **Exhibit 10**. A true and correct copy of the Certificate of Default is attached hereto as **Exhibit 11**.

10. On February 15, 2022, I was contacted by Igor Litvak, now counsel of record for Defendants Dmitry Starovikov and Alexander Filippov (collectively, "Defendants").[1] A true and correct copy of Mr. Litvak's email is attached hereto as **Exhibit 12**. Mr. Litvak stated that the Defendants would "consent to personal jurisdiction in this matter." He requested that Google consent to set aside the Certificate of Default and consent to Defendants' request to file an Answer to Google's Complaint. Mr. Litvak's email represents the first time Defendants or any of their representatives attempted to contact Google since the Complaint was unsealed on December 7, 2021, *see* ECF Nos. 4, 5.

11. I spoke with Mr. Litvak on February 17, 2022. He noted that he expected to be retained by both Defendants but had not yet been formally retained by Mr. Filippov. He again stated that Defendants would consent to personal jurisdiction. He also stated that Defendants were interested in settling the dispute and would be able to provide Google with assistance and information to permanently disrupt and dismantle the botnet in exchange for Google's agreement to set aside the Clerk's Certificate of Default. I requested details concerning the type of "cooperation" Defendants could offer and the legal and factual basis as to why Defendants or their

[1] On February 17, 2022 and February 21, 2022, Mr. Litvak filed Notices of Appearance on behalf of Defendant Starovikov and Defendant Filippov, respectively. *See* ECF Nos. 39, 40.

counsel believed the Certificate of Default should be set aside. Mr. Litvak agreed to confer with his clients and stated that he would follow up to provide any information his clients could offer. I replied that Google would be willing to review any information Defendants could provide regarding the botnet or the "cooperation" Defendants might be able to offer.

12. On Tuesday, February 22, 2022, Mr. Litvak emailed stating that his clients were "not ready" to discuss "any potential cooperation right now." Mr. Litvak did not elaborate on any details regarding potential cooperation from Defendants and stated that Defendants "would like to file a motion to set aside the Notice of Default, and then, if it's successful, . . . work on everything else, discovery, settlement, potential cooperation, etc." He further stated that if Google were "willing to set aside the notice of default voluntarily," the case could proceed to "discovery, cooperation, and settlement much faster." Ex. 12 at 2.

13. On Thursday, February 24, 2022, Defendants, through Mr. Litvak, filed a motion requesting that the Court suspend the then-existing schedule so that Defendants could move to vacate the Clerk's Entry of Default. *See* ECF No. 41.

14. The Court held a conference on March 1, 2022, at which Defendants again stated that they would consent to personal jurisdiction in this case and that, if the Court suspended the schedule and allowed their request to vacate the Certificate of Default, they would file an Answer and would not move to dismiss. A true and correct copy of the transcript from the March 1, 2022 conference is attached hereto as **Exhibit 13**.

III. Service of Process

15. I oversaw Google's efforts to provide service and notice to the Defendants through the multiple channels identified below. As set forth in my declaration in support of the TRO Application, Ex. 8, ECF No. 24, ¶ 8, prior to the TRO filing, Google's Threat Analysis Group

("TAG") conducted an investigation to identify the true identities of all persons responsible for operating the Glupteba botnet.

16. This investigation revealed contact information associated with each Defendant—in particular, the physical mailing addresses, email addresses, and telephone numbers associated with Defendants and/or the entities, IP addresses, or domains under their control or otherwise associated with their criminal enterprise (the "Enterprise") or the Glupteba botnet. Defendants themselves provided certain of this information to Google and/or web hosting companies and domain registrars used by the Enterprise. This information was used by Google to attempt to effectuate service on Defendants by (a) physical mail, (b) email, and (c) text messages.

a. Service by Mail

17. Google attempted to effectuate service by physical mail.

18. On December 8, 2021 at 6:00 pm ET, Google attempted to serve Defendants by FedEx at the following physical address that Google identified as being associated with Defendants through TAG's pre-filing investigation:

Dmitry Starovikov
123112, Moscow, Presnenskaya
Embankment 12, Office 5

Alexander Filippov
123112, Moscow, Presnenskaya
Embankment 12, Office 5

19. On December 21, 2021, FedEx issued a notification that it was unable to deliver the shipment to the address. As of February 7, 2022, FedEx labeled the shipments "undeliverable."

b. Service by Email

20. Google also attempted to effectuate service by email, as authorized by the TRO. The Court specifically provided that "good cause continues to exist to grant alternative service of

the filings in this matter via . . . email . . . because Google establishes that traditional service methods would be futile." Ex. 4, ECF No. 8, ¶ 18.

21. Google identified multiple email addresses associated with Defendants in its pre-filing investigation. Defendants have used these email addresses in registering the domains associated with the botnet.

22. I oversaw the process of sending notice of this lawsuit to each of the email addresses identified by Google in its pre-filing investigation. Each email attempting to effectuate service was sent by an attorney at King & Spalding with the following text:

> A lawsuit has been initiated against you in the United States District Court of the Southern District of New York. The following link contains copies of the restraining order, summons and complaint.
>
> https://drive.google.com/drive/folders/1bGIIKRQmgoVbh93t0JiGAKi-f2Dbiof3?usp=sharing
>
> Regards,
> King & Spalding LLP

23. King & Spalding attempted to effectuate service by email, as described above, on December 8, 2021, at approximately 9:00 pm ET.

24. On December 10, 2021, at approximately 4:00 pm ET, King & Spalding further attempted to notify Defendants by email that the "hearing on the motion for a preliminary injunction" had been "adjourned to 1 pm ET on December 16, 2021" and provided a link to a copy of the Court's order.

25. King & Spalding received delivery failure notifications for each of its emails. In one such instance, King & Spalding received a message that its email had been "blocked . . . due to [an] organization setting."

c. Service by Text Message

26. Google also attempted to effectuate service by text message as authorized by the TRO. The Court specifically provided that "good cause continues to exist to grant alternative service of the filings in this matter via . . . text . . . because Google establishes that traditional service methods would be futile." Ex. 4, ECF No. 8, ¶18.

27. *Texts to Starovikov*: On December 9, 2021 at around 1:30 pm ET, and December 10, 2021 at 3:00 pm ET, I oversaw service of process by text message to a phone number associated with Defendant Starovikov, as identified through Google's pre-filing investigation. King & Spalding received an "invalid number" error message in response to these efforts.

28. On December 9, 2021 and December 10, 2021, King & Spalding also attempted to effectuate service on Defendant Starovikov by text message through the WhatsApp messaging platform—specifically, through an account connected to one of the telephone numbers associated with Starovikov. King & Spalding did not receive a delivery failure notification or an error message in response to its WhatsApp message.

29. *Texts to Filippov*: On December 9, 2021 at around 1:30 pm ET, and December 10, 2021 at 3:00 pm ET, I oversaw service of process by text messages to two numbers associated with Alexander Filippov, as identified through Google's pre-filing investigation. King & Spalding did not receive any delivery failure notifications or error messages in response to the text messages sent to these numbers.

30. Each of the text messages and WhatsApp messages sent to Defendants contained the following message: "A lawsuit has been filed against you in the United States District Court for the Southern District of New York. This link contains a copy of a restraining order, summons, and complaint." The text messages sent on December 10, 2021 also informed the Defendants that

the preliminary injunction hearing had been scheduled for December 16, 2021 and provided a link to a copy of the Court's order.

IV. Additional Means of Notification

31. Upon information and belief, and as discussed in my Declaration in Support Of Google's Request for Entry of Default, *see* ECF 36, ¶¶ 19–22, Defendants have actual notice of this proceeding given the impact of the TRO, the Preliminary Injunction Order, and Google's disruption efforts thereunder.

32. On or around December 13, 2021, Defendants ceased operating one of their most prominent storefronts, Dont.farm, which the Enterprise had used to sell access to stolen Google user account information. Managers of Dont.farm informed the storefront's customers that they were shutting down, and subsequently deleted the accounts that had been used to communicate with those customers. Dont.farm sent messages to its customers misrepresenting the reason for the shut-down, claiming that the issues experienced after Google's disruption efforts were "bugs" associated with an "update[]" to fix a "speed issue" on the Dont.farm platform. True and correct copies of Dont.farm's communications with its customers on December 8, 2021 and December 10, 2021 are attached hereto as **Exhibit 14**.

33. Numerous Russian-language news sites reported Google's lawsuit against Defendants, identified them by name, and detailed the allegations against them, including:

- TASS, the largest state-run news agency in Russia;[2]

[2] True and correct copies of the relevant article, *Google Filed a Lawsuit Against Two Russians Because of Possible Participation in a Criminal Scheme*, TASS (Dec. 7, 2021), https://tass.ru/ekonomika/13137081, are attached hereto in both the original Russian and an English Google Translation as **Exhibit 15**.

- BBC News Russia, part of BBC Worldwide News Service;[3]
- Gazeta.ru, a popular source of online news for Russian citizens (translates to "Newspaper.ru");[4]
- Novaya Gazeta, a well-regarded newspaper whose editor-in-chief shared the 2021 Nobel Peace Prize;[5]
- Tsargrad TV, a media organization that the U.S. State Department describes as pro-Kremlin;[6]
- RAPSI, the Russian news agency for legal news,[7] which also reported on subsequent developments in the case;[8]

---

[3] True and correct copies of the relevant article, *Two Russians and 15 Unknowns. Google Files Lawsuit Against Hackers Who Infected More than a Million Computers*, BBC NEWS RUSSIA (Dec. 8, 2021), https://www.bbc.com/russian/news-59569423, are attached hereto in both the original Russian and an English Google Translation as **Exhibit 16**.

[4] True and correct copies of the relevant article, Alexandra Vishnevskaya, *Google Accused the Russians of Infecting a Million Devices Worldwide with a Malicious Bot*, GAZETA.RU (Dec. 7, 2021), https://www.gazeta.ru/tech/news/2021/12/07/n_16979221.shtml, are attached hereto in both the original Russian and an English Google Translation as **Exhibit 17**.

[5] True and correct copies of the relevant article, *Google Files Lawsuit Against Two Russian Hackers for Creating a Botnet That Steals User Data*, NOVAYA GAZETA (Dec. 8, 2021), https://novayagazeta.ru/articles/2021/12/08/google-podala-isk-protiv-dvukh-rossiiskikh-khakerov-za-sozdanie-botneta-pokhishchaiushchego-dannye-polzovatelei-news, are attached hereto in both the original Russian and an English Google Translation as **Exhibit 18**.

[6] True and correct copies of the relevant article, Nikolay Gyngazov, *American Company Believes That Two Russians Infected Millions of Computers Worldwide with a Virus*, TSARGRAD (Dec. 8, 2021), https://nn.tsargrad.tv/_news/amerikanskaja-kompanija-schitaet-chto-dvoe-rossijan-zarazili-virusom-milliony-kompjuterov-vo-vsjom-mire_459111, are attached hereto in both the original Russian and an English Google Translation as **Exhibit 19**; *see also* U.S. DEP'T OF STATE, *GEC Special Report: Pillars of Russia's Disinformation and Propaganda Ecosystem* (Aug. 2020), https://www.state.gov/wp-content/uploads/2020/08/Pillars-of-Russia%E2%80%99s-Disinformation-and-Propaganda-Ecosystem_08-04-20.pdf.

[7] True and correct copies of the relevant article, *Google Suspected Two Citizens of the Russian Federation of Administering the Glupteba Botnet*, RAPSI (Dec. 8, 2021), http://rapsinews.ru/international_news/20211208/307583785.html, are attached hereto in both the original Russian and an English Google Translation as **Exhibit 20**.

[8] True and correct copies of the relevant articles—*Google Notifies US Court of Blocking 97 Domains and IP Addresses in Glupteba Botnet Case*, RAPSI (Feb. 1, 2022) (covering Google's

- Govorit Moskva, a Moscow local news website;[9]
- Moskovskaya Gazeta, a Moscow local news website;[10]
- Habr, a popular internet blog akin to Reddit;[11]
- Afisha Daily, a popular culture and events website;[12]
- Esquire Russia, associated with the men's fashion magazine;[13] and

---

Jan. 31, 2022 status letter), http://rapsinews.ru/international_news/20220201/307697396.html; *US Court May Consider Petition for Default Judgment in Glupteba Botnet Case*, RAPSI (Feb. 11, 2022) (covering Google's request for default judgment), http://rapsinews.ru/international_news/20220211/307719520.html—are attached hereto in both the original Russian and an English Google Translation as **Exhibit 21 and 22**, respectively.

[9] True and correct copies of the relevant article, *Google Filed a Lawsuit Against Two Russians Because of Possible Participation in a Criminal Scheme*, GOVORIT MOSKVA (Dec. 7, 2021), https://govoritmoskva.ru/news/297591, are attached hereto in both the original Russian and an English Google Translation as **Exhibit 23**.

[10] True and correct copies of the relevant article, *Google Accused the Russians of Infecting a Million Devices Worldwide with a Malicious Bot*, MOSKOVSKAYA GAZETA (Dec. 7, 2021), https://moskovskaya-gazeta.ru/hitech/google-obvinila-rossiian-v-zarajenii-milliona-ystroistv-po-vsemy-miry-vredonosnym-botom/, are attached hereto in both the original Russian and an English Google Translation as **Exhibit 24**.

[11] True and correct copies of the relevant article, Annie Bronson, *Google Sues Two Russians for Creating a Botnet That Infected More than a Million Windows PCs Worldwide*, HABR (Dec. 7, 2021), https://habr.com/ru/news/t/594039/, are attached hereto in both the original Russian and an English Google Translation as **Exhibit 25**.

[12] True and correct copies of the relevant article, Denis Lamekhov, *Google Sued Two Russians. They Are Suspected of Managing a Botnet That Attacked Yandex*, AFISHA DAILY (Dec. 8, 2021), https://daily.afisha.ru/news/57661-google-podal-v-sud-na-dvoih-rossiyan-ih-podozrevayut-v-upravlenii-botnetom-atakovavshim-yandeks/, are attached hereto in both the original Russian and an English Google Translation as **Exhibit 26**.

[13] True and correct copies of the relevant article, *Google Is Suing a Group of Hackers for Creating a Botnet That Has Infected More than a Million Computers. Among the Accused Are Two Russians*, ESQUIRE RUSSIA (Dec. 8, 2021), https://esquire.ru/news/society-news/08-12-2021/307323-google-podala-v-sud-na-gruppu-hakerov-za-sozdanie-botneta-zarazivshego-bolee-milliona-kompyuterov-sredi-obvinyaemyh-dvoe-rossiyan/, are attached hereto in both the original Russian and an English Google Translation as **Exhibit 27**.

- Rambler, a Russian search engine and news aggregator.[14]

34. In the very unlikely event that Defendants Starovikov and Filippov did not come across one of the above articles themselves—or were not alerted to them by any of their family, friends, or associates—there was also extensive coverage in the niche affiliate marketing and cryptocurrency communities in which Defendants participate, including on the Black Hat World Forum, of which Dont.farm was a member. A staff member of the Black Hat World Forum also publicly stated on December 15, 2021 that he had "informed" Dont.farm of the allegations in the lawsuit, and that Dont.farm's "ad account" was frozen. A true and correct copy of excerpted discussions on Black Hat World Forum from December 15, 2021 is attached as **Exhibit 29**.

35. Several Russian black hat affiliate marketing blogs covered the lawsuit in detail, including referencing the Defendants by name.[15] Likewise, the Russian-language cryptocurrency website Crypto News wrote about the lawsuit,[16] as did two Russian malware-focused news

---

[14] True and correct copies of the relevant article, *Google Accuses Russians of Infecting More than 1 Million Computers and Creating an "Invincible" Hacker System*, RAMBLER (Dec. 8, 2021), https://news.rambler.ru/internet/47725123-google-obvinil-rossiyan-v-zarazhenii-bolee-1-milliona-kompyuterov-i-sozdanii-nepobedimoy-hakerskoy-sistemy/, are attached hereto in both the original Russian and an English Google Translation as **Exhibit 28**.

[15] True and correct copies of the relevant articles—*Cloud Account Service Dont.Farm Announced Its Closure*, AFFTIMES (Dec. 13, 2021), https://afftimes.com/news/dontfarm/ (stating that the blog attempted to reach out to Dont.farm representatives, who refused comments and then deleted their Telegram messaging accounts); *Why Dont.farm and ExtraCard Closed*, PROTRAFFIC (Dec. 13, 2021), https://protraffic.com/news/dontfarmrip-45187.html; *Dont.farm and Extracard Are Closed: What Happened and What Should Affiliates Prepare For*, CPA LIVE (Dec. 13, 2021), https://cpalive.pro/dont-farm-i-extracard-zakryty-chto-sluchilos-i-k-chemu-gotovitsya-arbitrazhnikam—are attached hereto in both the original Russian and an English Google Translation as **Exhibits 30, 31, and 32**, respectively.

[16] True and correct copies of the relevant article, *Hidden Miners in the Java Library and Google's Accusations*, CRYPTO NEWS (Dec. 13, 2021), https://cryptonews.net/ru/news/security/2878371/, are attached in both the original Russian and an English Google Translation as **Exhibit 33**.

websites, Anti-Malware and Security Lab.[17] And on Twitter, the lawsuit was covered in depth by CoinDesk,[18] a cryptocurrency news service that has 2.7 million followers, and by Brian Krebs,[19] a prominent cybercrime investigative reporter with over 344,200 followers.

V. Defendants' Actions in the United States

36. Dont.farm sold access to stolen accounts in the United States as part of its "premium" service. A true and correct copy of Dont.farm's black hat marketing brochure, accessed on November 2, 2021, is attached hereto as **Exhibit 36**.

37. AWMProxy.net also sold access to proxies from infected devices in the United States. A true and correct copy of AWMProxy.net's "Proxies by Country" page, accessed on November 2, 2021, is attached hereto as **Exhibit 37**.

VI. Defendants' Ongoing Conduct

38. Defendants will continue to participate in cybercriminal activities through the Glupteba Enterprise. Defendants' actions to reconstitute the Enterprise in the wake of Google's disruption efforts include repeated attempts to infect new devices with the Glupteba botnet, establish new C2 servers, and resume other criminal schemes. All of these actions will continue

---

[17] True and correct copies of the relevant articles—Ekaterina Bystrova, *Google Accuses Two Russians of Creating a Powerful Glupteba Botnet*, ANTI-MALWARE (Dec. 8, 2021), https://www.anti-malware.ru/news/2021-12-08-111332/37692; *Google Sued 17 People, Including Two Russians*, SECURITYLAB.RU (Dec. 8, 2021), https://www.securitylab.ru/news/527277.phphttps://www.securitylab.ru/news/527277.php—are attached in both the original Russian and an English Google Translation as **Exhibits 34 and 35, respectively**.

[18] CoinDesk (@CoinDesk), TWITTER (Dec. 7, 2021, 11:06AM), https://twitter.com/CoinDesk/status/1468250656494559237.

[19] Brian Krebs (@briankrebs), TWITTER (Dec. 7, 2021, 12:27PM), https://twitter.com/briankrebs/status/1468270834758430722.

to cause harm to Google, its customers, and the public.

VII. Damages

39. Google's Complaint sought a judgment awarding (i) actual damages, (ii) enhanced, exemplary, and special damages, and (iii) attorneys' fees and costs, *see* ECF No. 5 (Prayer for Relief, G–I). Google has withdrawn its request for monetary damages in connection with its motion for Default Judgment and a Permanent Injunction.

VIII. State Department Travel Warning

40. A true and correct copy of the State Department's warning to United States citizens regarding their travel to Russia is attached hereto as **Exhibit 38**.

In accordance with 28 U.S.C. § 1746, I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge

Executed on March 25, 2022 in New York, New York.

/s/ Laura Harris
Laura Harris